УДК 004

ПРИКЛАД ОНТОЛОГІЧНОЇ СТРУКТУРИ АНАЛІЗУ СЦЕНАРІЇВ ВИТОКУ ІНФОРМАЦІЇ ТА РІВНЯ КУЛЬТУРИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

О. В. Козленко[1]

[1] *Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Фізико-технічний інститут*

Анотація

У статті пропонується застосування онтологічної структури для аналізу КСЗІ, яка орієнтована на найбільш поширені варіанти сценаріїв витоку інформації та на певний рівень культури інформаційної безпеки організації. Аналіз КСЗІ зважає на багато факторів. Це, зокрема, сценарії атак на інформаційну систему організації, програмні помилки та помилки персоналу, невчасне реагування на інциденти безпеки, стан культури інформаційної безпеки організації та інше. Загалом оцінка рівня інформаційної безпеки організації потребує проведення складного аналітичного дослідження, що спирається на застосування чіткої формалізованої концептуальної схеми. Запропоновано методологію формування цієї схеми, в основу якої покладено онтологію предметної області, візуально представлену онтографом.

Ключові слова: онтологічна структура, оцінювання ризику, сценарії витоку інформації, культура інформаційної безпеки, онтограф, загрози інформації, рівень культури інформаційної безпеки

Вступ

Забезпечення надійного захисту інформації потребує значних коштів. Тому перед впровадженням захисних заходів потрібно впевнитися у їх доцільності. Зокрема, збереження конфіденційних даних для багатьох компаній є одним з головних пріоритетів у веденні успішного бізнесу, а інформація про конкурентів може допомогти побудувати свій бізнес-план таким чином, щоб випередити їх на декілька кроків. В загальному випадку витік даних може призвести не тільки до значних фінансових втрат, але й до повного розпаду організації. Для її захисту від витоків інформації або інших інформаційних загроз потрібно провести повний аналіз захищеності інформаційних систем срганізації. Цей аналіз спирається на різноманітні методи та заходи, наприклад, дослідження сценаріїв витоку інформації, інше. Одночасно потрібно враховувати адміністративні аспекти захисту інформації, такі як обізнаність персоналу про загрози інформації у системі. Тому для оцінювання, наприклад, значення середнього ризику витоку інформації потрібно враховувати багато факторів, їх взаємозв'язків та взаємозалежностей. В цьому випадку побудова та візуалізація структури, що містить визначені фактори, сценарії, взаємозв'язки й т.п., буде значно спрощувати розуміння та автоматизацію цих розрахунків для їх подальшого використання. Окрім того, безпека організації залежить не тільки від технічних засобів. Звичайні помилки та нерозуміння наслідків інцидентів безпеки, вчасної та адекватної реакції на них теж відіграють важливу роль. Дана робота фокусується на демонстрації онтологічної структури, яку можна використовувати для побудови та аналізу комплексних систем захисту інформації (КСЗІ) системи, та подальшого визначення загальної формальної оцінки захищеності організації та автоматизації процесу визначення цієї оцінки.

1. Теоретичні основи побудови онтології предметної області

Процес побудови КСЗІ у зв'язку з необхідністю високого рівня деталізації її структури, зокрема, виділення головних складових елементів, впливових факторів, відношень між ними вимагає для аналізу та дослідження цієї структури застосування чіткої формалізованої концептуальної схеми. Якраз такі особливості властиві таким структурам як «онтології». Серед фахівців, що займаються проблемами комп'ютерної лінгвістики, найбільш усталеним (класичним) вважається визначення онтології, дане Грубером: «Онтологія – це специфікація концептуалізації» [1]. Так само відомий ряд розширених визначень Грубера, серед яких можна виділити такі:

1) Онтологія – це специфікація концептуалізації, де в якості концептуалізації виступає опис множини об'єктів предметної області та зв'язків між ними [2];
2) Онтологія – це знання, формально представлені на базі концептуалізації. Формально онтологія складається з термінів, організованих в таксономії їх визначень і атрибутів, а також пов'язаних з ними аксіом і правил поведінки [2];

Також є складності з формальним визначенням поняття «онтологія». Згідно [3] комп'ютерна онтологія

предметної області (Пдо) це трійка: $O = < X, R, F >$, де $X = \{x_1, x_2, \ldots, x_i, \ldots, x_n\}$, i=$\overrightarrow{1n}$, $n = CardX$ - кінцева множина понять заданої предметної області; $R = \{r_1, r_2, \ldots, r_k, \ldots, r_m\}$, $R = x_1 * x_2 * \ldots * x_n$, $k = \overrightarrow{1m}$, $n = CardR$ – кінцева множина семантично значущих відносин між концептами Пдо і визначають тип взаємодії між поняттями. $F = X * R$ – кінцева множина функцій інтерпретації, заданих на X або R. Хоча вищезазначені множини і складають онтологію, але найбільш зручно зображати онтологію у виді онтографу. Онтограф – односпрямований орієнтований граф в одну вершину якого може входити і виходити кілька дуг, де вершинами є поняття предметної області, а дугами – зв'язки між ними. У простому випадку методика проектування онтології Пдо включає три етапи:

- Попередній аналіз заданої предметної області.
- Побудова вручну онтографа Пдо.
- Графічне (візуальне) проектування онтографа Пдо.

Як можна побачити, перший етап у проектуванні онтології («попередній аналіз предметної області»)є найбільш важливим, тому що на цьому етапі визначаються основні терміни і відношення між ними. Для побудови онтології для аналізу КСЗІ потрібно провести аналіз сценаріїв витоку інформації для розуміння можливих елементів захисту та аналіз адміністративного аспекту захисту інформації.

2. Сценарії витоку інформації

Аналіз інформаційних систем є складним процесом и включає в себе багато інших операцій. Однією з складових аналізу інформаційних систем є визначення елементів КСЗІ. Для визначення елементів захисту системи від витоку інформації потрібно знати можливі загрози для цільової системи та відповідно необхідні дії захисту. Згідно [4] дії, які призводять до реалізації потенційних небезпек, що ведуть до зниження цінності інформаційних ресурсів і мають потенційно можливий несприятливий вплив називаються загрозами, а спроба реалізації загрози називається атакою. Компанія Verizon щорічно проводить дослідження [5, 6] і вже не перший рік доводить доцільність поділу інцидентів витоку даних на дев'ять сценаріїв. Для побудови онтології, призначеної для аналізу комплексних систем захисту інформації, необхідно розглянути кожний з цих сценаріїв окремо:

- Сценарій «Вторгнення в точки продажу» включає в себе атаки на середовища, де проводяться роздрібні торгові операції, зокрема розрахунки картками.
- Сценарій «Атаки на веб-застосунки» включає у себе випадки з зловмисним кодом, спрямованим на вразливості рівня машинних команд у додатках або зривом механізмів автентифікації.
- До сценарію «Злочинне ПЗ» належать всі випадки заволодіння секретною інформацією за допомогою програм зловмисників, за виключенням випадків атак на точки продажу та на веб-застосунки.
- Під «Кібер-шпигунством» розуміються всі інциденти, де мав місце неправомірний доступ до систем та мереж, пов'язаний з мотивом заволодіння чужою інформацією та/або мотивом шпигунства.
- В сценарій «Скимери платіжних карток» входять пристрої, фізично встановлені у місця зчитування даних з магнітних стрічок платіжних карток, метою яких є збір та підробка даних та незаконне втручання у платіжні операції.
- До сценарію «Фізична крадіжка або втрата» належать випадки крадіжки або загублення через неуважність фізичних носіїв інформації.
- В сценарій «Різні помилки» входять випадки ненавмисного компрометування атрибутів безпеки інформаційних активів, що не підходять під інші названі сценарії.
- Будь-яка атака, спрямована на порушення доступності мережі або системи належить до сценарію «DOS – атак». Як правило, такі інциденти в результаті не порушують конфіденційність.
- Сценарій «Інсайдерських атак» охоплює всі інциденти, які сталися через те, що внутрішні працівники або довірені особи зловживали своїми правами чи свідомо недбало виконували свої обов'язки.

3. Культура інформаційної безпеки

Суттєвий вплив на інформаційну безпеку організації становить людський фактор, який не завжди пов'язаний з нестачею або недосконалістю заходів захисту, але завжди пов'язаний з недотриманням вимог політики безпеки (ПБ). Як і раніше, організації страждають від випадкових або навмисних помилок співробітників, незважаючи на наявність політики безпеки і необхідних технологій. Як зазначається у [7] є два можливих вирішення питання про недотримання вимог:

- Реалізація суворої системи перевірки, яка визначає систему штрафів і дисциплінарних заходів у разі недотримання. Це рішення дає швидкі результати, хоча негативне її сприйняття співробітниками робить ефект нетривалим.
- Розробка високого рівень культури інформаційної безпеки (КІБ). Варіант досить довгостроковий, але має тривалий ефект у разі успіху.

Згідно [8] КІБ визначається показниками «Персонал» та «Керівництво». Індикатор «Персонал» визначається нижчими показниками «Кадрова безпека» і «Міра прийняття КБ», «Керівництво» – «Управлінська готовність» та «Координованість». Індикатор «Координованість» аналогічним чином визначається показниками нижчими рівня «Співпраця з відділом ІБ» і «Співпраця з менеджментом». Ці показники й будуть використовувати у подальшого аналізі і побудові досліджуваної онтологічної структури.

4. Онтологія предметної області

Побудуємо онтологічну структуру для аналізу КСЗІ, беручи за основу матеріали по вищезазначеним сценаріям по витоку інформації і рівню культури ІБ та опираючись на методику побудови онтології. Першим етапом є «Попередній аналіз заданої предметної області». Для цього потрібно зробити визначення множин X та R. Отже множина понять X буде мати вигляд: { Центр безпеки, Секретні дані, Політика безпеки, КІБ, Захист від витоку інформації, Персонал, Керівництво, Атаки на веб-застосунки, DoS – атаки, Інсайдерські атаки, Різні помилки, Фізична крадіжка або втрата, Скимери платіжних карток, Кібер-шпигунство, Злочинне ПЗ, POS вторгнення, Управлінська готовність, Координованість, Співпраця з відділом ІБ, Співпраця з менеджментом, Кадрова безпека, Міра прийняття КБ, Захист від шкідливого ПЗ, Фільтрування трафіку, Журнал подій, Протокол NetFlow, Подвійна автентифікація, Контроль адмінів, Відокремлення серверів, Паролі, Інвентарізація ПЗ, Чорні та білі IP списки, Конфігурація, Обізнаність співробітників, Сегментація мережі, Оновлення та патчі, Відео спостереження, Перевірка терміналів, Попередження користувачів, Ефективний дизайн, Резервне копіювання, Шифрування, DLP – Система, Відсутність секретних даних у відкритому тексті, Журнал подій, Управління аккаунтами, Відповіді на інциденти, Безпека розробки }. Множина відношень R складається з відношень { Ціле-частина, Визначає, Використовує }. Наступним етапом є «Побудова вручну онтографа Пдо». Для цього виконуємо ранжування списку термінів по узагальненому відношенню «вище – нижче».

1) Центр безпеки
2) Секретні дані, Політика безпеки, КІБ.
3) Захист від витоку інформації, Персонал, Керівництво.
4) Атаки на веб-застосунки, DoS – атаки, Інсайдерські атаки, Різні помилки, Фізична крадіжка або втрата, Скимери платіжних карток, Кібер-шпигунство, Злочинне ПЗ, POS вторгнення, Управлінська готовність, Координованість.
5) Співпраця з відділом ІБ, Співпраця з менеджментом, Кадрова безпека, Міра прийняття КБ, Захист від шкідливого ПЗ, Фільтрування трафіку, Журнал подій, Протокол NetFlow, Подвійна автентифікація, Контроль адмінів, Відокремлення серверів, Паролі, Інвентарізація ПЗ, Чорні та білі IP списки, Конфігурація, Подвійна автентифікація, Обізнаність співробітників, Сегментація мережі, Інвентарізація ПЗ, Оновлення та патчі, Відео спостереження, Перевірка терміналів, Попередження користувачів, Ефективний дизайн, Резервне копіювання, Шифрування, DLP – Система, Журнал подій, Управління аккаунтами, Відсутність секретних даних у відкритому тексті, Відповіді на інциденти, Безпека розробки.

На рис. 1 та рис. 2 зображено остаточний онтограф системи для аналізу КСЗІ.

Висновки

В роботі були проаналізовані сценарії витоку інформації, отримані із звітів щодо витоку інформації у 2014, 2015 роках та особливості культури інформаційної безпеки, яка має відношення до загроз, пов'язаних з людськими чинниками. В результаті проведеного аналізу було визначено необхідні множини та відношення для побудови онтологічної структури. Отримана онтологічна структура (онтограф) системи для аналізу КСЗІ враховує можливі сценарії витоку інформації, визначені дослідженням даних щодо інцидентів в області інформаційної безпеки та з врахуванням специфіки культури інформаційної безпеки. Цей онтограф може використовуватися як основа, яку можна застосовувати для аналізу КСЗІ системи для подальшого визначення загальної формальної оцінки захищеності організації та, як приклад, автоматизації процесу визначення цієї оцінки, який базуватиметься на використанні отриманого онтографу.

Перелік використаних джерел

1. Gruber T. R. A translation approach to portable ontologies Knowledge Acquisition. — 1993. — № 5(2). – 199 – 220с.
2. Никоненко А. А. Обзор баз знаний онтологического типа «Искусственный интеллект» — 2004. — № 4. – 208 – 219 с.
3. Палагин А. В., Петренко Н. Г. Методика проектирования онтологии предметной области // УСиМ. — 2009. — 14 с.
4. Архипов О. Є. Щодо методики ідентифікації та оцінювання активів системи інформаційних технологій / О. Є. Архипов // Захист інформації. — 2011. – № 1 (50). — с.42 – 47.
5. 2015 Data Breach Investigation Report, Verizon Enterprise Solutions, 2015.
6. 2014 Data Breach Investigation Report, Verizon Enterprise Solutions, 2014.
7. A. V. Potiy, D. Y. Pilipenko, I. N. Rebriy The prerequisites of information security culture development and an approach to complex evaluation of its level — 2012. – № 5 (57). — с.72 – 77.
8. Майерс Д. Социальная психология «Искусственный интеллект» — 1997. — СПб.: Питер, 1997. – 688 с.

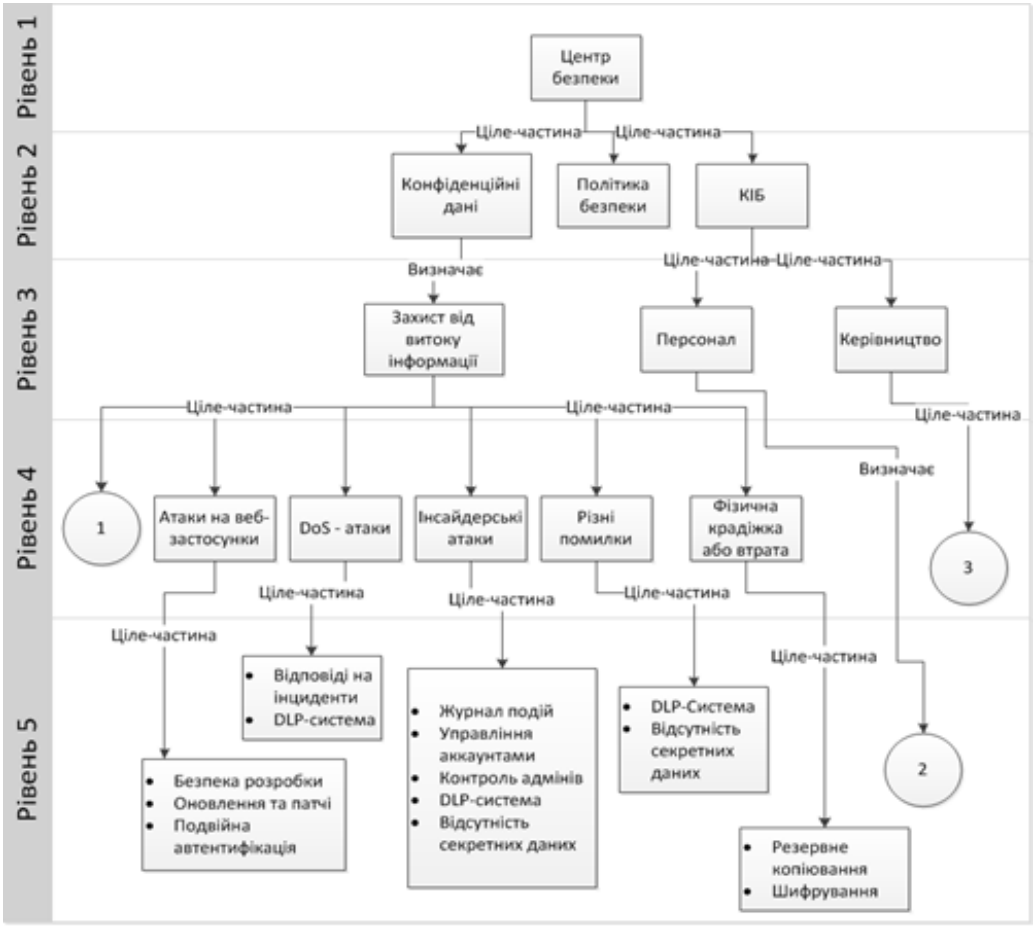

Рис. 1. Онтограф. Частина 1

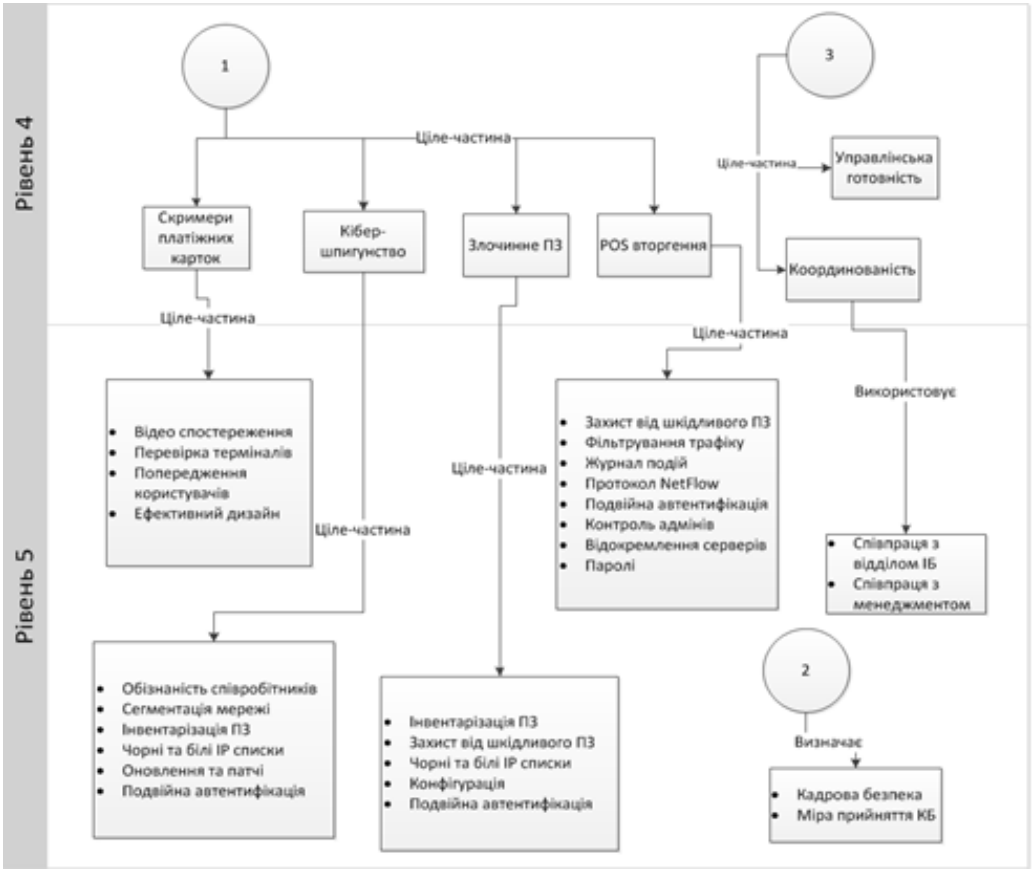

Рис. 2. Онтограф. Частина 2